Data Protection Policy

Introduction

The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but Power2 must respect their right to have control over their personal data and ensure it always acts in full compliance with legislative and regulatory requirements. If individuals feel that they can trust the charity as a custodian of their personal data, this will also help Power2 to fulfil its wider objectives.

The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), is the main piece of legislation that governs how Power2 collects and processes personal data. Failure to comply with this legislation may have severe consequences for the charity, including potential fines of up to £17.5 million or 4% of Power2's total annual turnover, whichever is higher.

Aims and Objectives

This Policy sets out how Power2 will process the personal data of its staff, beneficiaries, suppliers and other third parties. This Policy applies to all personal data that the charity processes regardless of the format or media on which the data are stored or who it relates to.

The policy also sets out the data controlled by Power2, how individuals can access their data and our retention and storage processes.

Policy Statement

Power2 is committed to processing data in accordance with its responsibilities under the DPA 2018. The DPA requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals.
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals.
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Additionally, Power2 must ensure that:

- Personal data is not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place.
- The charity allows data subjects to exercise their rights in relation to their personal data.

Power2 is responsible for, and must be able to demonstrate compliance with, all of the above principles.

Responsibilities

Power2 shall comply with the principles of data protection enumerated in the GDPR. We will make every effort possible in everything we do to comply with these principles.

Power2's responsibilities are:

- Analysing and documenting the type of personal data we hold.
- Checking procedures to ensure they cover all the rights of the individual.
- Identify the lawful basis for processing data.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report and investigate personal data breaches.
- Store data in safe and secure ways.
- Assess the risk that could be posed to individual rights and freedoms should data be compromised.
- Test contingency plans at least once a year. The IT security issues we will respond to are:
    - Malware infection detected by scanners
    - Ransomware
    - System failure
    - Attempted social engineering
    - Data loss or theft

Responsibilities of the named **Data Protection Officer (DPO)**:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders.
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us.
- Checking and approving with third parties that handle the charity's data any contracts or agreement regarding data processing.

Responsibilities of the **IT Manager**:

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the charity is considering using to store or process data.

Responsibilities of the **Communications Manager**:

- Approving data protection statements attached to emails and other marketing copy.

- Addressing data protection queries from clients, target audiences or media outlets.
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the charity's Data Protection Policy.

Employees (including volunteers) responsibilities are:

- Fully understand your data protection obligations.
- Check that any data processing activities you are dealing with comply with our policy and are justified.
- Do not use data in any unlawful way.
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions.
- Always comply with this policy.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy without delay to the Data Protection Officer.

Everyone who handles data is responsible for helping maintain good practice in protecting personal information. To help us do this Power2 requires everyone working with us or representing us to comply with the following:

Disposal of equipment and documents

1. confidential waste will be shredded and disposed of in designated bins.
2. hard drives will be removed and manually destroyed when computers are no longer in service.

Laptops

1. individual computers will be locked (ctrl alt delete) when users are not at their desk or when visitors may have sight of screens.
2. computer screens will be turned away from windows or from areas where they may be viewed by people who are not entitled to view them.
3. confidential information will be accessed through designated drives and not sent as email attachments or otherwise removed from the building.

Mobile devices

1. mobile devices will be password protected, have timed screen locks in place and not be left unattended. If using fingerprint or facial recognition, another alphanumerical password must be set. These passwords will be stored centrally by HR.
2. care will be taken when using open networks (WiFi) to send or open emails.

File storage

- files will be stored electronically on encrypted systems and/or cloud servers and will not be saved to the desktop, on personal pen drives or other storage devices.
- paper documents, where these are necessary, will be stored in locked cabinets in secured buildings and not left unattended at any time.
- files (electronic and paper) will not be removed from the building unless prior authorisation has been given by the designated manager.
- Multifactor authentication will be used wherever possible.

Passwords

- single sign-on passwords will be used to minimise the risk of users writing passwords down.

- passwords will have a minimum of eight characters combining numerals, letters and symbols and will not include partial names or other identifying information.
- passwords will be changed every 90 days.
- passwords for mobile devices must include an alphanumeric password that is shared with HR to be stored centrally.
- Wherever possible, Power2 will make use of multifactor authentication.

Internet use

- only users with system administrator rights may download information or attach hardware to the charity's computers.
- downloading of shareware is never permitted.
- any unauthorised, illegal, pornographic or offensive material opened, shared, displayed or accessed will result in immediate withdrawal of user access, is likely to be a disciplinary offence and may result in criminal prosecution use of social networks is prohibited except for designated user(s) (e.g. a media/communications person might operate a Power2 twitter account).

Enforcement

It is in everyone's interest to adhere to good basic security practices. All members of staff have an obligation to report actual or potential data protection compliance failures. Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Power2 has a legal obligation to report any data breaches.

The immediate reporting of any breach or near-miss allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures.

Failure to protect an individual's privacy can have serious consequences for the charity, its people and its supporters. Fines of up to £500,000 may be issued by the Information Commissioner's Office www.ico.org.uk or claims for damages may be brought through the courts by individuals who are harmed through careless management of personal information.

In the event of a data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Any data security incident which occurs due to an intentional disregard of this policy, whether for the means of releasing data or not, will be investigated as a disciplinary matter. Power2 will support prosecution where a criminal charge is brought against any individual. Power2 reserve the right to recover any loss, arising through breach of confidence, through the civil court. On the termination of employment, for whatever reason, the employee's user accounts will be cancelled and their rights of access to the IT system removed.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.
Please refer to the breach form for our reporting procedure.

Power2 take compliance with this policy very seriously. Failure to comply puts both you and the charity at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. Breaches of this policy will be dealt with under the charities Disciplinary Procedure.

Lawful Basis

All data processed by the charity must have a lawful basis established for us to process the data. Ensure that any data you are responsible for managing has a lawful basis approved by the DPO. It is the employee's responsibility to check the lawful basis for any data they are working with and ensure all their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent -** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract -** The processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation -** We have a legal obligation to process the data (excluding a contract).
4. **Vital interests -** Processing the data is necessary to protect a person's life or in a medical situation.
5. **Public function -** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. **Legitimate interest -** The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Personal data is information which, either on its own or when combined with other information held by the charity, identifies a living individual. It includes their name, home address or email address and birth details. We maintain data privacy through:

1. encrypted technology.
2. information handling processes.
3. people's behaviour.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

Consent forms for young people will set out the agencies with whom we may share information in the best interests of the young person, as well as those who may be contacted in more exceptional circumstances.

Careful consideration will be given to whether new information received from external parties needs to be included on an individual's file.

Procedure to determine lawful basis

If you are assessing the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means. Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest. Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to our data protection Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose and fully justify these decisions. We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice (see appendix 1). This applies whether we have collected the data directly from the individual, or from another source.

Withdrawing Consent

Power2 must always inform individuals of their right to object to their data being processed or withdraw consent at the first point of communication, i.e. in the privacy notice. Individuals have the right to object to their data being used on grounds relating to their particular situation and request that it is erased in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed.
- Where consent is withdrawn.
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with a legal obligation.
- The processing relates to a child.

Power2 can only refuse to comply with an erasure request in the following circumstances:

- There are legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

Transparency

We must ensure accountability and transparency in our use of all personal data. We must show how we comply with each Principle. To comply with data protection laws and the accountability and transparency principle of GDPR, we must demonstrate compliance. Employees are

responsible for understanding their particular responsibilities to ensure the charity meets the following data protection obligations:

- Fully implement all appropriate technical and organisational measures.
- Maintain up to date and relevant documentation on all processing activities.
- Conducting Data Protection Impact Assessments.
- Implement measures to ensure privacy by design and default, including:
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security and enhanced privacy procedures on an ongoing basis.

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. Data subjects have the right to have any data unlawfully processed erased.

Power2 is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling and processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller.
- Co-operate fully with the ICO or other supervisory authority.
- Ensure the security of the processing.
- Keep accurate records of processing activities.
- Notify the controller of any personal data breaches.

Special categories of personal data

This means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any

such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

Power2 recognises that automated decision-making and profiling, including the use of AI tools, can have significant implications for individuals. AI must not be used to make decisions that affect individuals' rights or opportunities without human oversight and prior approval from the DPO. Individuals retain the right to:

- Object to automated processing, including AI-driven profiling.
- Request an explanation of the rationale behind any AI-assisted decision.
- Request human intervention in any decision-making process involving AI.

Use of Artificial Intelligence (AI)

Power2 supports the responsible use of Artificial Intelligence (AI) to enhance productivity and efficiency. The charity currently authorises Microsoft Copilot and Fathom (for meeting notetaking) as the primary approved AI tools.

Conditions for AI use:

- AI outputs must be checked by yourself before being used in any capacity.
- AI must not be used for automated decision-making that affects individuals without prior approval from the Data Protection Officer (DPO).

If for some reason it is necessary to use an AI tool that it is not Microsoft Copilot or Fathom it must be approved by the DPO and must follow these guidelines:

- Wherever possible the AI must be used in privacy mode.
- All data input must be anonymised; no personal data, sensitive information, or confidential details may be entered, including charity name.
- Prompts should be generic and task-focused.
- All outputs must be checked for accuracy and compliance before publication.

Prohibited uses

- Uploading or typing names, addresses, health data, or any personally identifiable information.
- Using AI for profiling or decisions that impact employment, beneficiaries, or service delivery without explicit authorisation.

Good Practice for AI Prompts

There are many ways of prompting AI, Power2 recommends that all staff use the CARE framework:

- Context
- Action
- Result
- Example

Any prompt should be clear and specific: State the task and context without including personal identifiers.

Examples:

I am a marketing manager looking to get more traffic to my website. I only have 1 hour a day to create and promote on social media so time is short. I want you to be the greatest copywriter ever to have lived (Context). Create a blog post on generative AI for charities of around 500 words (Action). Use the AIDA framework, make it SEO friendly therefore included H1 and H2 tags as well as relevant keywords (Result). Include some bullet points and a call to action. I want it to come across as not too formal but sounding professional (Example).

Monitoring & Compliance:

Use of AI tools will be periodically reviewed by the DPO. Breaches of this section will be treated as data protection violations and may result in disciplinary action.

Data Recording and Storage

During its day-to-day activities Power2 has access to a wide variety of personal information about individuals. This information is needed to enable the organisation to carry out its charitable work with young people and to manage people who work for and represent the charity (employees, volunteers, trainees, mentors and contractors).

Power2 has specific legal responsibilities, under the Data Protection Act 2018, to protect personal information it holds on individuals. The charity also recognises the rights of individuals not to have unnecessary invasions of privacy under the Human Rights Act. As well as having a legal right to privacy, people have reasonable expectations about how information they provide will be used. Power2 will only keep information that is needed for some specified purpose.

The Charity shall ensure that personal data is stored securely using modern software that is kept up to date. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information. You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the named DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations. When personal data is deleted, this should be done safely such that the data is irrecoverable and in accordance with the record retention and disposal policy.

In instances where Power2 makes uses of cloud servers the provider will be ISO27001 compliant as a minimum and levels of access applied ie. employees will only be able to access data required for their job.

Data Classification

Internally, as far as possible, we operate on a '**need to share'** rather than a 'need to know' basis with respect to charity confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

As for client information, we operate in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format. We also allow data subjects to transmit their own personal data to another controller.

However, in general, to protect confidential information we implement the following access controls:

Charity confidential

- Xero – limited to 2 users, Accountant and the Director of Finance.
- Charity server – access to directories is controlled by sharing rights. Staff are allocated to groups with access to certain files shares. Changes are approved only by gatekeepers (3 staff).

Client confidential

- Xero – limited to 2 users, Accountant and the Director of Finance.
- Charity server – access to directories is controlled by sharing rights. Staff are allocated to groups with access to certain files shares. Changes are approved only by gatekeepers (3 staff).
- Salesforce – data limited by hierarchical access structure of rights according to user type. Only 4 admin users with overall rights.

Beneficiary Confidential

- Xero – limited to 2 users, Accountant and the Director of Finance.
- Charity server – access to directories is controlled by sharing rights. Staff are allocated to groups with access to certain files shares. Changes are approved only by gatekeepers (3 staff).
- Salesforce – data limited by hierarchical access structure of rights according to user type. Only 4 admin users with overall rights.
- Paper files are kept locked with keys limited to 3 staff.

Employee confidential

- Xero – limited to 2 users, Accountant and the Director of Finance.
- Charity server – access to directories is controlled by sharing rights. Staff are allocated to groups with access to certain files shares. Changes are approved only by gatekeepers (3 staff).
- Breathe – data limited by hierarchical access structure of rights according to user type. Only 1 admin user with overall rights.
- Paper files are kept locked with keys limited to 3 staff.

Power2 will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- **Unclassified:** this is information that can be made public without any implications for the charity, such as information that is already in the public domain.
- **Employee confidential:** this includes information such as medical records, pay and so on.
- **Charity confidential:** such as contracts, source code, business plans, passwords for critical IT systems, staff mobile devices passwords, client contact records, accounts etc.
- **Client confidential:** this includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.
- **Beneficiary Confidential:** this includes data about young people. Some of this is sensitive personal data, such as safeguarding concerns. This policy is designed to minimise that risk.

We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.

Power2 have categorised the information we keep as follows:

Type of Information	**Systems Involved**	**Classification Level**
Student data	Salesforce, server	Beneficiary confidential
Safeguarding concerns	Server	Beneficiary confidential

Staff	Xero, Salesforce, server, Breathe	Employee confidential
Clients	Xero, Salesforce, server	Client confidential
Funder records	Xero, Salesforce, server	Client confidential
Supplier records	Xero, server	Charity confidential

Using third-party controllers and processors

As a data controller and a data processor, we must have written contracts in place with any third-party data controllers and data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a **data controller**, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a **data processor**, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR, and we will protect and respect the rights of data subjects.

Information Sharing

When it is necessary to share information, the following is a good summary and set of rules that should be followed:

- The Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- Seek advice if you are in any doubt, without disclosing the identity of the person where possible.
- Share with consent where appropriate and, where possible respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
- Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
- Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
- Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

The flowchart in appendix 2 shows the key questions for information sharing.

<u>Safeguarding</u>

Sharing information between organisations is a vital part of keeping children safe, agencies (such as schools, local authorities and the police) can only act quickly and effectively when they hold the right information at the right time. When safeguarding breaks down, it is often because key information wasn't shared early enough or wasn't shared with the people who needed it.

The ICO is clear that data protection law should never be a barrier to safeguarding. If a child is at risk, you can and should share the relevant information with the appropriate professionals. Power2 safeguards children and young people by sharing concerns and relevant information with authorised agencies who need to know and who will manage and respond to the concern appropriately. The safeguarding form will e password protected and the password shared in a separate email.

Data retention
We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Storage
In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it. Printed data should be shredded when it is no longer needed.

Data stored on a computer should be protected by strong passwords that are changed regularly and multifactor authentication implemented wherever possible. We encourage all staff to use a password manager to create and store their passwords. Data should be regularly backed up in line with the charity's backup procedures. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones. All possible technical measures must be put in place to keep data secure.

All servers containing sensitive data must be approved and protected by security software that is compliant with ISO27001 as a minimum.

Contracts
Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with [data controllers (and/or) data processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions.
- Those involved in processing the data are subject to a duty of confidence.
- Appropriate measures will be taken to ensure the security of the processing.
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract.
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR.
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments.
- Delete or return all personal data at the end of the contract.
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Security

A security incident is defined as any incident which results in the unauthorised disclosure of confidential or sensitive information. It includes a near-miss where the potential for unauthorised disclosure is high although there is no actual disclosure or loss of data. Most security breaches are the result of human error rather than malevolent acts and the risk of an actual breach can be significantly reduced by changes in human behaviour. Power2 will review its risk register regularly to ensure all potential serious risks are appropriately logged and categorised.

It may also include 'protected disclosure' under public interest legislation, procedural or other suspected incident of non-compliance with legislation and regulation as well as potential breach of confidence.

Security Incidents have potentially serious consequences which include:

1. compromise to the dignity and personal privacy of individuals with whose information the charity is entrusted.
2. damage to the charity's reputation.
3. inability of the charity or its representatives to meet its contractual and other obligations.
4. financial penalties arising from imposition of fines for statutory breaches or claims for damages.

Near misses are incidents where no actual breach has occurred but the potential for a breach is more than remote. Examples may include:

- leaving confidential or sensitive information unattended in semi-secure environments.
- writing down passwords or door entry codes.
- persistent failure to lock secure information away overnight.
- careless electronic transactions including failing to check recipient list when responding to or forwarding emails.
- discussing confidential matters in places where there is the potential for eavesdropping.

All security incidents will be reported to the named Data Protection Officer using the Breach Notification Form. Notification to the Senior Management Team and IT department will be according to the classification of the information involved. Serious incidents will always be reported to the Chief Executive who will alert the Board of Trustees and manage external communications. Security incident prevention will be monitored within the charity's performance management arrangements and form part of the supervision arrangements. Training and guidance will be provided, particularly when there are changes to systems or processes.

An assessment will determine the seriousness of the incident and whether such incident is classified as Level 1 or Level 2. Level 2 incidents are the more serious. All breaches must be reported, initially, to a senior manager as soon as possible after the incident has occurred and in any case within eight hours of the incident.

An assessment will cover:

1. the type of information involved.
2. the scale of the breach/loss.
3. the circumstances of the breach (i.e. whether it was an accidental loss or an intentional incident such as a hack or deliberate release).
4. whether any individuals have been placed at risk.
5. whether there is a risk to part or the whole of the organisation.

6. whether responsibility for the breach can be identified.

When a security incident has occurred, dependent upon the classification, further action may include:

- informing individuals about the loss of their personal data to allow them to take any remedial action.
- informing parties to a contract if an incident affects the charity's compliance with that contract.
- review of contract terms, where an incident is caused by a facilitator or independent contractor.
- notification to regulatory authorities: Information Commissioner's Office [ICO], social care regulators, the Financial Services Authority, the Fundraising Standards Board.
- report to police or other investigation bodies.
- notification to others to manage potential risks or damage to the charity or others.
- review of procedures/security levels to reduce the risk of recurrence.
- implementation of performance improvement or disciplinary processes.

Activities, or attempted activities, which represent an intentional data breach which will automatically be classified as a Level 2 breach and therefore a fundamental breach of contract. Examples include, but are not limited to:

- unauthorised access to data or information or providing the means of such access to others, regardless of intent.
- access to data for purposes other than those permitted.
- intentional or reckless release of data, including
- selling, publication or disclosure through social networking email, or to individuals within the organisation who are not authorised to have access to it.
- destruction, corruption unauthorised deletion, modification or introduction of software or malware.
- any other activity prohibited by law including the Data Protection Act (2018), Computer Misuse Act (1990), any breach of communications or other legislation or regulations or codes of practice.
- any other unauthorised and intentional activity which breaches or endangers the security of data.

Portable Data Media

Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being
used.

The named DPO must approve any cloud software used to store data.

Protecting device(s)

It is also the responsibility of staff to use devices (computer, phone, tablet etc.) in a secure way. However, we will provide support to enable you to do so. At a minimum:

- Remove software that you do not use or need from your computer.
- Update your operating system and applications regularly
- Keep your computer firewall switched on.
- For Windows users, make sure anti-malware software is installed (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software.

- Store files in official charity storage locations so that it is backed up properly and available in an emergency.
- Switch on whole disk encryption.
- Make use of multifactor authentication wherever possible.
- Understand the privacy and security settings on your phone and social media accounts.
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.
- Don't use an administrator account on your computer for everyday use.
- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.

Transfers Outside the European Economic Area (EEA)

The GDPR prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

Power2 may only transfer personal data outside of the EEA if one of the following conditions applies:

- the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries).
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission, an approved code of conduct or certification mechanism which, in each case, can be obtained from the Information Governance Manager and named Data Protection Officer.
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks.
- the transfer is necessary in order to perform a contract between the charity and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent.
- the transfer is necessary, in limited circumstances, for Power2's legitimate interests.

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that the charity has agreed to this in advance.

Right of Access

Individuals have a right under the Data Protection Act to receive confirmation that their data is being processed, access to their personal data or challenge information the charity holds about them. A formal request to view files is known as a 'subject access request' and must be complied with unless there is a genuine risk of harm, or a third party, who has not given consent, may be identified.

Power2 must provide an individual with a copy of the information requested, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible,

provide direct access to the information through a remote accessed secure system. On receiving a request to view a personal file, a manager with responsibility for data protection will go through the file to ensure that sensitive or third-party information is removed, and a note is attached saying that this has been done.

Power2 must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the named DPO before extending the deadline.

Power2 can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the named DPO. Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Accuracy and relevance

Power2 will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the named DPO.

Training

All staff will receive adequate training on provisions of data protection law specific to their role. Staff must complete all training as requested, if a member of staff moves role or responsibilities, they are responsible for requesting new data protection training relevant to the new role.

If any member of staff requires additional training on data protection, they should contact the named DPO.

Review

Everyone must observe this policy. The named DPO has overall responsibility for this policy, and it will be monitored and reviewed every three years by the Senior Management Team, or earlier if the legislation changes.

You must notify the named DPO of any breaches of this policy and you must always comply with this policy fully.

Related Policies

This policy should read in conjunction with the following Power2 policies:

- Safeguarding policy

- Digital and social media policy
- Consent policy
- Business continuity plan
- Record retention and disposal policy
- Safer recruitment and selection policy

This policy has been drawn up based on the following legislation and guidance:

- Data Protection Act DPA 2018
- Computer Misuse Act 1990
- The General Data Protection Regulation
- ICO guidance

Approval

This policy has been considered and approved by the Senior Management Team.

Julie Randles
Chief Executive
5 January 2026

Appendix 1 - Privacy notices

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how
    - those decisions are made, their significances and consequences to the data subject
    - Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

If you are responsible for assessing the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the named DPO.

Appendix 2 – Information Sharing Key Questions